REMARKS

In response to the Office Action mailed June 6, 2008 and the Advisory Action mailed August 22, 2008, Applicants respectfully request reconsideration. To further the prosecution of this Application, Applicants submit the following remarks and have cancelled claims. The claims as now presented are believed to be in allowable condition.

Claims 1, 2, 4-28, and 38-45 were pending in this Application. By this Amendment, claim 39 has been cancelled and claim 38 amended to include the content of cancelled dependent claim 39. Also by this amendment, claims 1 and 40 were amended to include the content of claim 9 as initially filed with the Application and as previously examined. Support for the amendment can be found in the Specification, for example, on page 6, line 30 through page 7, line 2. Additionally, claim 16 has been rewritten in independent form. These amendments do not add new matter to the Application. Accordingly, claims 1, 2, 4-28, 38, and 40-45 are now pending in this Application. Claims 1, 9, 16-19, 38, 40, 41, 43 and 45 are independent claims.

Allowed Claims

Claims 9 and 10 have been allowed. The Applicants would like to thank Examiner Jeffery Williams for his indication as to the allowance of claims 9 and 10.

Claim 16 was objected to as being dependent on a rejected base claim but was deemed allowable if rewritten in independent form to include all of the limitations of the base claim and any intervening claims. Claim 16 has been rewritten in independent form to include the content of the base claim (i.e., claim 1) and any intervening claims. Accordingly, claim 16 as amended is in a condition for allowance.

Rejections under §101

Claims 38 and 39 were rejected under 35 USC §101 because the claimed invention is directed to non-statutory subject matter. The Office Action recites that "[r]egarding claims 38 and 39, these claims comprise essentially computer instructions upon a readable medium such as carrier waves. As such, such claims are rejected for not being tangible."

Claim 38 has been amended to recite an article comprising a tangible machine readable medium that stores executable code instructions. Further more, claim 39 has been cancelled and claim 38 amended to include the content of cancelled dependent claim 38. The amendments do not add new matter to the application. Accordingly, because claim 38 is directed to non-statutory subject matter, the rejection of claim 38 under 35 USC §101 should be withdrawn.

Rejections under §102 and §103

Claims 1, 2, 4-8, 11, 12, 14-15, 17-28, and 38-45 were rejected under 35 U.S.C. §102(b) as being anticipated by "A Fuzzy Commitment Scheme" (hereinafter Juels). Applicants respectfully traverse each of these rejections and request reconsideration. The claims are in allowable condition.

Claims 1 and 40 were rejected under 35 U.S.C. §102(b) as being anticipated by Juels. As indicated above, claims 1 and 40 were amended to include the content of previously-examined claim 9 as initially filed with the Application. Specifically, claims 1 and 40 as ameded each relate to a computer-implemented method for creating an order- invariant fuzzy commitment and recite in part "reordering the first sequence based upon the first value."

Juels relates to a type of cryptographic commitment scheme, referred to as a fuzzy commitment scheme. Juels, page 28, paragraph 1. Juels describes

the fuzzy commitment scheme as "meaning that the commitment scheme should be resilient to small corruptions in witness values." Juels, page 29, paragraph 2.

While claims 1 and 40 were rejected under 35 U.S.C. §102(b) as being anticipated by Juels, claims 1 and 40 as amended are patentable over Juels because Juels does not teach or suggest all of the elements of claims 1 and 40. For example, Juels does not teach or suggest method for creating an order-invariant fuzzy commitment that includes "reordering the first sequence based upon the first value" as claimed by the Applicants.

As indicated above, Jules does indicate that the fuzzy commitment scheme is resilient to small corruptions in witness values, Juels is silent as to a computer-implemented method for creating an order- invariant fuzzy commitment that includes "reordering the first sequence based upon the first value" as claimed by the Applicant in claims 1 and 40 as amended.

For the reasons stated above, claims 1 and 40 as amended patentably distinguish over the cited prior art, and the rejection of claims 1 and 40 under 35 U.S.C. §102(b) should be withdrawn. Accordingly, claims 1 and 40 are in allowable condition. Because claims 2-8 and 11-15 depend from and further limit claim 1, claims 2-8 and 11-15 are in allowable condition for at least the same reasons.

Claim 17 was rejected under 35 U.S.C. §102(b) as being anticipated by Juels. Claim 17 relates to a computer-implemented method for decommitting an order-invariant fuzzy commitment comprising receiving a first input element including a sequence of one or more values from a predetermined set, receiving an order-invariant fuzzy commitment sequence, constructing a set of integers having a predetermined number of elements representing respectively values in the first input element, selecting a subset of the coordinate sets in the first

sequence such that the first value in each subset coordinate set corresponds to the first value of at least one coordinate set in the first sequence, applying an error-correcting function to the subset, and outputting the subset.

The Office Action, on pages 3-6, provides its reasoning for the rejection of claims 1, 2, 4-8, and 11-15. With respect to the rejection of claim 17, the Office Action asserts, on page 6, that "[r]egarding claims 17-28, and 38-45, they comprise essentially similar limitations, and they are rejected, at least for the same reasons as the claims above." The Applicants respectfully disagree with such an assertion.

As indicated above, claim 17 relates to a computer-implemented method for decommitting an order-invariant fuzzy commitment and recites in part "receiving an order-invariant fuzzy commitment sequence." While the Office Action indicates that such a recitation "comprise[s] essentially similar limitations" as claims 1, 2, 4-8, and 11-15, none of claims 1, 2, 4-8, and 11-15 recite a computer-implemented method for decommitting an order-invariant fuzzy commitment that includes "receiving an order-invariant fuzzy commitment sequence" as claimed by the Applicants in claim 17. If the rejection of claim 17 is to be maintained, Applicants respectfully request that it be pointed out with particularity where the cited prior art teaches a computer-implemented method for decommitting an order-invariant fuzzy commitment that includes "receiving an order-invariant fuzzy commitment sequence" as claimed by the Applicants in claim 17.

Claim 18 was rejected under 35 U.S.C. §102(b) as being anticipated by Juels. Claim 18 relates to a computer-implemented method for creating a reordering-tolerant fuzzy commitment comprising receiving a first input element A including a first sequence of at least one value, generating a first codeword c of an error-correcting code for the commitment, constructing a sequence E of one

or more data elements responsive to the first input element A and the error-correcting code c, outputting the sequence E, receiving a second input element B including a second sequence of at least one value and the sequence E, wherein the second sequence has a number of elements m, applying a function d responsive to the second input element B and the sequence E, wherein the function yields as output a value of a second codeword (c' d(B,E)), the function having a property such that d(V,E) =c for at least one possible value of V, where V comprises a third sequence having a number of elements m_v, wherein the at least one value of the first sequence differs from the at least one value of the third sequence in at least m_v /2 values, and outputting the second codeword c'.

With respect to the rejection of claim 18, the Office Action indicates that claim 18 "comprise[s] essentially similar limitations" as claims 1, 2, 4-8, and 11-15. However, none of claims 1, 2, 4-8, and 11-15 recite a computer-implemented method for creating a reordering-tolerant fuzzy commitment that includes "applying a function d responsive to the second input element B and the sequence E, wherein the function yields as output a value of a second codeword (c' d(B,E)), the function having a property such that d(V,E) =c for at least one possible value of V, where V comprises a third sequence having a number of elements m_v, wherein the at least one value of the first sequence differs from the at least one value of the third sequence in at least m_v /2 values" as claimed by the Applicants in claim 18. If the rejection of claim 18 is to be maintained, Applicants respectfully request that it be pointed out with particularity where the cited prior art teaches a computer-implemented method for creating a reordering-tolerant fuzzy commitment that includes "applying a function d responsive to the second input element B and the sequence E, wherein the function yields as output a value of a second codeword (c' d(B,E)), the function having a property such that d(V,E) =c for at least one possible value of V, where V comprises a third sequence having a number of elements m_v, wherein the at least one value

of the first sequence differs from the at least one value of the third sequence in at least $m_v/2$ values" as claimed by the Applicants in claim 18.

Claim 19 was rejected under 35 U.S.C. §102(b) as being anticipated by Juels. Claim 19 relates to a computer-implemented method for generating an order invariant fuzzy commitment of an item of information, comprising receiving a first set of elements, selecting a polynomial for encoding the item under the first set of elements to generate an order-invariant fuzzy commitment of the item, and storing said commitment in a computing device.

With respect to the rejection of claim 19, the Office Action indicates that claim 19 "comprise[s] essentially similar limitations" as claims 1, 2, 4-8, and 11-15. However, none of claims 1, 2, 4-8, and 11-15 recite a computer-implemented method for generating an order invariant fuzzy commitment of an item of information that includes "selecting a polynomial for encoding the item under the first set of elements to generate an order-invariant fuzzy commitment of the item" and "storing said commitment in a computing device" as claimed by the Applicant in claim 19. If the rejection of claim 19 is to be maintained, Applicants respectfully request that it be pointed out with particularity where the cited prior art teaches a computer-implemented method for generating an order invariant fuzzy commitment of an item of information that includes "selecting a polynomial for encoding the item under the first set of elements to generate an order-invariant fuzzy commitment of the item" and "storing said commitment in a computing device" as claimed by the Applicants.

Claim 39 (i.e., claim 38 as amended) was rejected under 35 U.S.C. §102(b) as being anticipated by Juels. Claim 38 as amended relates to an article comprising a machine readable medium that stores executable code instructions enabling a machine to perform the steps of receiving a first input element comprising a sequence of at least one value from a predetermined set,

generating a codeword of an error-correcting code, and constructing a first sequence of coordinate sets, each of the coordinate sets having a first value corresponding to a representation of an associated one of the at least one value of the first input element and a second value corresponding to a symbol in the codeword, wherein the symbol is associated with the corresponding first value. Claim 38 as amended further recites including code for enabling the steps of receiving a second input element including a second sequence of at least one value from the predetermined set, receiving the order-invariant fuzzy commitment, constructing a set of values representing respectively the values in the second sequence, selecting a subset of the coordinate sets in the first sequence such that the first value in each subset coordinate set corresponds to the first value of at least one coordinate set in the first sequence; and applying an error-correcting function to the subset.

With respect to the rejection of claim 38 as amended, the Office Action indicates that claim 38 "comprise[s] essentially similar limitations" as claims 1, 2, 4-8, and 11-15. However, none of claims 1, 2, 4-8, and 11-15 recite an article comprising a machine readable medium that stores executable code instructions for enabling the step of "receiving the order-invariant fuzzy commitment" as claimed by the Applicant in claim 38 as amended. If the rejection of claim 38 as amended is to be maintained, Applicants respectfully request that it be pointed out with particularity where the cited prior art teaches an article comprising a machine readable medium that stores executable code instructions for enabling the step of "receiving the order-invariant fuzzy commitment" as claimed by the Applicants

Claim 41 was rejected under 35 U.S.C. §102(b) as being anticipated by Juels. Claim 41 relates to a computer-implemented method for creating an order-invariant fuzzy commitment, comprising receiving a first input element (A) comprising a sequence of at least one value (a_1,..., a_n) from a predetermined set

(F), generating a codeword (c) of an error-correcting code for generating the commitment, constructing a first sequence (E) of coordinate sets (x_i,z_i,y_i), for i in {1,…,k} for integer k > 0, each of the coordinate sets having a first value (x_i) corresponding to a representation of an associated one (a_i) of the at least one value of the first input element (A) and a second value (z_i) constructed in a manner responsive to a pattern of occurrence of the associated one (a_i) of the at least one value of the first input element (A) in the sequence $(a_1,..., a_n)$ and a third value (y_i) corresponding to a subset of symbols in the codeword (c), wherein the subset of symbols is selected in a manner responsive to at least one of the first and second values of the coordinate set (x_i and z_i), wherein an order-invariant fuzzy commitment is formed and outputting the first sequence.

With respect to the rejection of claim 41, the Office Action indicates that claim 41 "comprise[s] essentially similar limitations" as claims 1, 2, 4-8, and 11-15. However, none of claims 1, 2, 4-8, and 11-15 recite a computer-implemented method for creating an order-invariant fuzzy commitment that includes ", constructing a first sequence (E) of coordinate sets (x_i,z_i,y_i), for i in {1,…,k} for integer k > 0, each of the coordinate sets having a first value (x_i) corresponding to a representation of an associated one (a_i) of the at least one value of the first input element (A) and a second value (z_i) constructed in a manner responsive to a pattern of occurrence of the associated one (a_i) of the at least one value of the first input element (A) in the sequence $(a_1,..., a_n)$ and a third value (y_i) corresponding to a subset of symbols in the codeword (c), wherein the subset of symbols is selected in a manner responsive to at least one of the first and second values of the coordinate set (x_i and z_i), wherein an order-invariant fuzzy commitment is formed" as claimed by the Applicants. If the rejection of claim 41 is to be maintained, Applicants respectfully request that it be pointed out with particularity where the cited prior art teaches such a computer-implemented method as claimed by the Applicants.

Claim 43 was rejected under 35 U.S.C. §102(b) as being anticipated by Juels. Claim 43 relates to a computer-implemented method for creating an order-invariant fuzzy commitment, comprising receiving a first input element (A) comprising a sequence of at least one value (a_1,. . ., a_n) from a predetermined set, generating a codeword (c) of an error-correcting code for generating the commitment, constructing a first sequence (E) of coordinate sets (x_i,z_i,y_i), for i in {1 ,...,k} for integer k > 0, each of the coordinate sets having a first value (x_i) corresponding to a representation of an associated one (a_i) of the at least one value of the first input element (A) and a second value (z_i) constructed in a manner responsive to information in the first input element (A), and a third value (y_i) corresponding to a subset of symbols in the codeword (c), wherein the subset of symbols is selected in a manner responsive to at least one of the first and second values (x_i and z_i) of the coordinate set, wherein an order-invariant fuzzy commitment is formed, and outputting the first sequence.

With respect to the rejection of claim 43, the Office Action indicates that claim 43 "comprise[s] essentially similar limitations" as claims 1, 2, 4-8, and 11-15. However, none of claims 1, 2, 4-8, and 11-15 recite a computer-implemented method for creating an order-invariant fuzzy commitment that includes "constructing a first sequence (E) of coordinate sets (x_i,z_i,y_i), for i in {1 ,...,k} for integer k > 0, each of the coordinate sets having a first value (x_i) corresponding to a representation of an associated one (a_i) of the at least one value of the first input element (A) and a second value (z_i) constructed in a manner responsive to information in the first input element (A), and a third value (y_i) corresponding to a subset of symbols in the codeword (c), wherein the subset of symbols is selected in a manner responsive to at least one of the first and second values (x_i and z_i) of the coordinate set, wherein an order-invariant fuzzy commitment is formed" as claimed by the Applicants. If the rejection of claim 43 is to be maintained, Applicants respectfully request that it be pointed out with particularity where the cited prior art teaches such a computer-implemented

method for creating an order-invariant fuzzy commitment as claimed by the Applicants.

Claim 45 was rejected under 35 U.S.C. §102(b) as being anticipated by Juels. Claim 45 relates to a computer-implemented method for creating an order-invariant fuzzy commitment, comprising receiving a first input element (A) comprising a sequence of at least one pair of values (a_1,w_1), (a_2,w_2),,..., (a_n,w_n) wherein each of the at least one a_i values is from a first predetermined set (F) and each of the at least one w_i values is from a second predetermined set (G), generating a codeword (c) of an error-correcting code for generating the commitment, constructing a first sequence (B) of coordinate sets (x_i,z_i,y_i), for i in $\{1,\ldots,k\}$ for integer $k > 0$, each of the coordinate sets having a first value (x_i) corresponding to a representation of an associated one $((a_i,w_i))$ of the at least one pair of values of the first input element (A) and a second value (z_i) constructed in a manner responsive to an associated one $((a_i,w_i))$ of the at least one value of the first input element (A) in the sequence (a_1,w_1), (a_2,w_2),,..., (a_n,w_n) and a third value (y_i) corresponding to a subset of symbols in the codeword (c), wherein the subset of symbols is selected in a manner responsive to at least one of the first and second values of the coordinate set (x_i and z_i), wherein an order-invariant fuzzy commitment is formed and outputting the first sequence.

With respect to the rejection of claim 45, the Office Action indicates that claim 45 "comprise[s] essentially similar limitations" as claims 1, 2, 4-8, and 11-15. However, none of claims 1, 2, 4-8, and 11-15 recite a computer-implemented method for creating an order-invariant fuzzy commitment that includes "constructing a first sequence (B) of coordinate sets (x_i,z_i,y_i), for i in $\{1,\ldots,k\}$ for integer $k > 0$, each of the coordinate sets having a first value (x_i) corresponding to a representation of an associated one $((a_i,w_i))$ of the at least one pair of values of the first input element (A) and a second value (z_i) constructed in a manner responsive to an associated one $((a_i,w_i))$ of the at least one value of the first input

element (A) in the sequence (a_1,w_1), (a_2,w_2),,..., (a_n,w_n) and a third value (y_i) corresponding to a subset of symbols in the codeword (c), wherein the subset of symbols is selected in a manner responsive to at least one of the first and second values of the coordinate set (x_i and z_i), wherein an order-invariant fuzzy commitment is formed" as claimed by the Applicants. If the rejection of claim 45 is to be maintained, Applicants respectfully request that it be pointed out with particularity where the cited prior art teaches such a computer-implemented method for creating an order-invariant fuzzy commitment as claimed by the Applicants.

For the reasons stated above, claims 17-19, 38, 41, 43 and 45 patentably distinguish over the cited prior art, and the rejection of claims 17-19, 38, 41, 43 and 45 under 35 U.S.C. §102(b) should be withdrawn. Accordingly, claims 17-19, 38, 41, 43 and 45 are in allowable condition. Because claims 20-28 depend from and further limit claim 19, claims 20-28 are in allowable condition for at least the same reasons. Because claim 42 depends from and further limits claim 41, claim 42 is in allowable condition for at least the same reasons. Because claim 44 depends from and further limits claim 43, claim 44 is in allowable condition for at least the same reasons.

Conclusion

In view of the foregoing remarks, this Application should be in condition for allowance. A Notice to this effect is respectfully requested. If the Examiner believes, after this Response, that the Application is not in condition for allowance, the Examiner is respectfully requested to call the Applicant's Representative at the number below.

Applicants hereby petition for any extension of time which is required to maintain the pendency of this case. If there is a fee occasioned by this Response, including an extension fee, please charge any deficiency to Deposit Account No. 50-3661.

If the enclosed papers or fees are considered incomplete, the Patent Office is respectfully requested to contact the undersigned collect at (508) 616-2900, in Westborough, Massachusetts.

Respectfully submitted,

/Jeffrey J. Duquette/

Jeffrey J. Duquette, Esq.
Attorney for Applicants
Registration No.: 45,487
Bainwood, Huang & Associates, L.L.C.
Highpoint Center
2 Connector Road
Westborough, Massachusetts 01581
Telephone: (508) 616-2900
Facsimile: (508) 366-4688

Attorney Docket No.: 1048-016

Dated: September 8, 2008